APEC e-Security Task Group Questionnaire on Spyware

Richard W. Downing
Senior Counsel
Computer Crime and Intellectual Property Section
U.S. Department of Justice

eSTG Spyware Questionnaire

- Report at the eSTG in Sept. 2004: spyware has increasingly become a problem
- Interest in doing further work in this area
- Questionnaire was proposed to help define the problem and survey what member economies have done to address it
- Report presented at eSTG meeting in April, 2005
eSTG Spyware Questionnaire

4 Questions:
- Identifying the attributes of “spyware”
- Scoping the problem
- Domestic initiatives to address the problem
- International work to address the problem


Discussion of the Questionnaire led to the proposal for a spyware workshop

Question 1:
Identifying the attributes of spyware

Very clear that there is no single accepted definition of spyware
- Some economies listed as many as 3 or 4 different definitions
Question 1: Identifying the attributes of spyware

Most definitions included some mix of the following factors:
- Software installed without the knowledge and consent of the user
- Software that secretly gathers information stored on or sent through the computer
- Software that secretly sends information back to a outside person
- Software that interferes with the computer’s functioning (such as by displaying ads or resetting “home pages”)

Some respondents supplied examples:
- Key loggers
- Data harvesters
- Navigation hijackers
- Tracking cookies
- Remote control tools
- Internet dialers

Important question raised by a number of respondents:
how to define spyware so that it includes the harmful or annoying aspects but avoids legitimate or beneficial software
Question 2: Scoping the Problem

- Varying perceptions of “level of threat”
- Most saw spyware as a growing problem
- Difficult to collect specific data on the incidence of spyware

Question 2: Scoping the Problem - Examples

- One report: 90% of Internet connected computers have some form of spyware
- Keylogging software that secretly gathered information on over 100,000 bank accounts
- Some perceive it to be more harmful than spam
- 2 companies reported that 10-12% of complaint calls to their call centers involved spyware
Question 3: Domestic initiatives to address the problem

Components of solving the problem:
- Technological improvements
- Consumer and industry education
- Criminal prosecution of worst types

Only some respondents advocated new laws and regulations. Worries include:
- Defining spyware
- Desirability of creating a unified policy on spam, phishing, malicious code in addition to spyware
- Much spyware comes from other economies

Need for a global response
- Some respondents pointed out that the Convention on Cybercrime (2001) already contains provisions that address some types of spyware
Question 4: 
*International work to address the problem*

- All respondents suggested that international work would help to address the problem
- International organizations can:
  - Help to define the problem
  - Assist in raising awareness
  - Provide a mechanism for discussion of governments’ role in addressing the problem

---

Question 4: 
*International work to address the problem*

- International law enforcement cooperation mechanisms can be used to help address the problem
- Coordination between international groups is important to avoid duplication
Questions?